UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/689,113	10/21/2003	Yair Buchsbaum		2906

44909 7590 12/06/2006

WOLF, BLOCK, SCHORR & SOLIS-COHEN LLP
250 PARK AVENUE
NEW YORK, NY 10177

EXAMINER	
HOANG, DANIEL L	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/689,113	BUCHSBAUM, YAIR	
	Examiner	Art Unit	
	Daniel L. Hoang	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/23/03, 5/25/05*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claims 4-9 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. See MPEP § 608.01(n). Proper correction is required. For purposes of examination, examiner will treat said claims as depending on claim 1, 2, or 3.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Frieder et al., US PGP No. 20030037251, hereinafter Frieder.

As per claim 1, Frieder teaches:

A method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user, comprising:

> *[see paragraph 4] "misuse is defined as use of a digital data gathering system by an authorized user which is permitted by the system but which is uncharacteristic, violates an internal security policy, or is otherwise out of the bounds of the intended use of the system."*

a) constructing a user and/or terminal profile representing a pattern of database's accesses;

> *[see paragraph 16] "adapted to build and maintain a profile of the behavior of the system user."*

b) monitoring user and/or terminal database access;

[see paragraph 16] "tracking, or monitoring, of user activity within the information retrieval system."

c) comparing the monitored database access' information with existing profile to determine anomalies and/or irregularities; and

[see paragraph 16] "compare each new use of the information retrieval system by the user to the user profile of previous behavior on the system."

d) identifying a potential misuse and/or abuse when an anomaly is detected.

[see paragraph 17] "Based on a user profile constructed by the present system, new queries and results are compared to the user profile and rated by the present system to cause the system to flag anomalous user behavior and, when necessary, to issue an alarm that potential misuse is indicated."

As per claim 2, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 1, further comprising:

a) comparing the anomalies to the user and/or terminal profile's parameters and grade it accordingly;

[see paragraph 25] "After a stabilization period in which a valid lexicon is developed representing typical user behavior, each new query submitted by the user will have the query terms or the key terms of the returned data, or both, compared to the lexicon."

b) reporting a potential misuse and/or abuse when the grade exceeds a predetermined threshold; and

[see paragraph 25] "Anomalous or infrequent query terms used, or returned with search results, or a threshold ratio of such query terms or results to typically used terms stored in the lexicon, may then be flagged or reported as an indication of potential misuse."

c) update profile according to comparison results and/or system owner instructions.

[see paragraph 77] "Structured data source queries performed by the user, or results of those queries, may also be monitored and cataloged to be added to the user profile or lexicon."

As per claim 3, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 2, further comprising:

a) constructing a profile for a group of users and/or terminals, representing a pattern of database's accesses related to that group;

> *[see paragraph 20] "Clustering is a technique whereby knowledge of a user's information retrieval searches is added to the user profile in the form of a cluster index which maintains the results of the user's searches according to topics, or families, describing the information or documents returned.*

b) comparing database access' parameters of a specific user and/or terminal with existing related group profile to determine anomalies and/or irregularities.

> *[see paragraph 21] "Cluster indexes deviating from this pattern of large and well-defined clusters potentially indicate misuse."*

As per claim 4, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 1-3, wherein

a) there is no need to understand and/or analyze the context of the actual data been manipulated and/or processed by a user; and b) the characteristics of each database access do not need to be predefined.

> *[see paragraph 20] "The returned documents are categorized or indexed to a topic structure, e.g., a family and genus structure, and the number of individual returns fitting into a particular family are counted and identified as a cluster. These few topics would normally be recognizably related to the user's search function although an automated system such as described typically need not know what the user's search function is."*

As per claim 5, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 1-3, wherein the parameters of a profile are:

a) commonly used statistics terms and/or any mathematical model and/or other figure or term, representing behavior and/or occurrence over any timeframe; and

> *[see paragraph 18] "a set of algorithms, or techniques, were developed to build a user profile and detect anomalies in user behavior compared against the user's profile which will indicate potential misuse of the data system. Each algorithm may independently flag certain anomalies. Together, the algorithms may be used to increase the likelihood of detecting a misuse."*

b) combine, part or all of: user identification, terminal and/or port identification, key characteristics of a database access, time stamp of the access.

[see paragraph 17] "There are essentially two fields with which the present system of tracking user behavior on an information retrieval system may operate: Input, or the query of the user which is used to obtain the information; and Output, or the data/information returned and made accessible by the information retrieval system."

As per claim 6, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 1-3, wherein the parameters and/or the depth of a profile are flexible and subject to a system owner's decisions with respect to time frames and levels of database segments.

[see paragraph 52] "After a stabilization period, that is, a time sufficient to establish a valid statistical threshold for family and genus clusters according to user search results, a results comparison function 47 will be instituted to compare the family/genus identifiers of each new search result against the cluster index."

[see paragraph 85] "Each of the techniques described above may be used singly or in various combinations. For example, an alarm might not be presented until each of the three techniques has indicated a potential misuse."

As per claim 7, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 1-3, wherein the related operations are executed in real-time, near real-time and/or on-line with the occurrence of database access, or off-line, batch mode and/or long after the actual access to database has been occurred.

[It is deemed inherent by the examiner that Frieder's operations are executed either in real-time, near-real time or after the access to the database occurs as it would be impossible to execute the operations before the actual access to the database occurs.]

As per claim 8, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 1-3, wherein the machines, servers and/or any related hardware of the data gathering system are singular or plural, distributed geographically and/or logically, and where database is singular or plural, distributed geographically and/or logically.

[It is inherent to the examiner that the machines, servers, and/or related hardware of the system taught by Frieder are either singular or plural as there must be at least one machine in which the information resides on. It is also clear that it is distributed geographically and/or logically.]

[see paragraphs 6 and 7] "There are two types of digital data gathering commonly in use. One, information retrieval, is concerned with the retrieval of information from unstructured data sources, such as text documents, where each element of the data is not individually defined. The second type of digital data gathering commonly in use is the structured data source search, where structured data, generally held to be identifiably correct, within one specific data source, usually privately owned and accessed."

As per claim 9, Frieder teaches:

The method for identifying a misuse and/or abuse of authorized access to a database of a data gathering system by a user according to claim 1-3, wherein a) the system owner can indicate specific segment/s within a database to be more sensitive than others and/or with predefined weight, for each desired segment, to be calculated accordingly in grading a warning or alarm; and/or b) the system owner can indicate specific user/s and/or terminal/s to be monitored and referenced with more sensitivity than others and/or with predefined weight, for each desired user or terminal, to be calculated accordingly in grading a warning or alarm.

[see paragraph 85] "Each of the techniques described above may be used singly or in various combinations. For example, an alarm might not be presented until each of the three techniques has indicated a potential misuse. If combined, the techniques could also be weighted or scaled according to a relative importance for a given employee classification."

CONCLUSION

The following patents and publications are cited to further show the state of the art with respect to misuse detection systems.

US Patent No. 555742 to Smaha et al., which is cited to show a method for detecting intrusion into and misuse of a data processing system.

US PGP No. 20030101260 to Dacier, which is cited to show a method for processing alarms triggered by a monitoring system.

US PGP No. 20030110398 to Dacier et al., which is cited to show a MDS with port logs.

US PGP No. 200300188191 to Aaron et al., which is cited to show a firewall system via feedback from broad-scope monitoring for intrusion detection.

US PGP No. 20050044406 to Stute, which is cited to show adaptive behavioral IDSs

US Patent No. 7124438 to Judge et al., which is cited to show a system for anomaly detection in patterns for monitored communications.

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DH

Daniel L. Hoang

11/20/06

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/21/06